AMENDMENTS TO THE CLAIMS

1.   (Currently Amended) A method comprising:

generating a list of update keys on a key distribution center system based on a

table of secret keys identifying the valid and invalid receivers of a

plurality of receivers, said list of update keys allowing valid receivers to

decrypt a valid content key using update keys obtained from the list of

update keys;

generating a multiple nested list of decryption patterns based on the list of update

keys;

broadcasting said multiple nested list of decryption patterns to the plurality of

receivers; and

recovering a content key from the list of update keys by recovering a set of update

keys for each receiver from the multiple nested list of decryption patterns

and using the set of update keys to decrypt the content key, wherein the

valid receivers receive the recovered content key to facilitate decryption of

content, and each of the invalid receivers receives a distinct intermediate

key to facilitate blocking of the content.

2.   (Currently Amended) The method of claim 1, wherein said generating a-of the list

of update keys comprises generating at least oneone or more distinct intermediate

key-keys and one-the content key.

3.   (Cancelled)

4.   (Cancelled)

5.   (Currently Amended) The method of claim 1, wherein said generating a~of the

multiple nested list of decryption patterns comprises encrypting an entry of the list

of update keys using a key that is a combination of a previous update key, a secret

key for a receiver associated with the entry of the list of update keys, and an index

indicating a location in said table of secret keys associated with each entry.

6.   (Currently Amended) The method of claim 5, wherein an entry in said multiple

nested list of decryption patterns includes a predetermined test pattern encrypted

with the secret keys~key for a~the receiver associated with the entry of the list of

update keys.

7.   (Currently Amended) The method of claim 1, wherein said recovering a~of the set

of update keys for each receiver from the multiple nested list of decryption

patterns comprises parsing said multiple nested list of decryption patterns to

locate an entry intended for a particular receiver based on detection of a

predetermined test pattern included in an entry in the multiple nested list of

decryption patterns.

8.   (Currently Amended) The method of claim 1, further comprising broadcasting

said content encrypted with said content key.

9.   (Original) The method of claim 8, further comprising decrypting said content encrypted with said content key using a content key recovered from the multiple nested list of decryption patterns.

Claims 10-18 (Cancelled)

19.   (Currently Amended) A system comprising:

a key distribution center to generate a list of update keys based on a table of secret keys identifying valid and invalid receivers of a plurality of receivers, said list of update keys allowing valid receivers of said plurality of receivers to decrypt a valid content key using update keys obtained from the list of update keys, generate a multiple nested list of decryption patterns based on the list of update keys, and broadcast said multiple nested list of decryption patterns to the plurality of receivers; and

a content receiver to recover an appropriate set of update keys from the multiple nested list of decryption patterns so that the final key recovered in the set of update keys is a content key, wherein the valid receivers receive the recovered content key to facilitate decryption of content, and each of the invalid receivers receives a distinct intermediate key to facilitate blocking of the content.

20.   (Currently Amended) The system of claim 19, wherein said key distribution center generates at least one or more distinct intermediate key keys and one the content key.

21.   (Cancelled)

22.   (Cancelled)

23.   (Original) The system of claim 19, wherein said key distribution center encrypts an entry of the list of update keys using a key that is a combination of a previous update key, a secret keys for a receiver associated with the entry of the list of update keys, and an index indicating a location in said table of secret keys associated with each entry to generate said multiple nested list of decryption patterns.

24.   (Cancelled)

25.   (Original) The system of claim 19, wherein said receiver parses said multiple nested list of decryption patterns to locate an entry intended for a particular receiver based on detection of a predetermined test pattern included in an entry in the multiple nested list of decryption patterns.

26.   (Currently Amended) The system of claim 19, further comprising a content provider to broadcast said content encrypted with said content key.

27.   (Cancelled)

28.   (Currently Amended) A machine-readable medium having stored thereon data representing ~~sequences~~ sets of instructions which, ~~the sequences of instructions which,~~ when executed by ~~a processor~~ machine, cause the ~~processor~~ machine to:

generate a list of update keys on a key distribution center system based on a table of secret keys identifying valid and invalid receivers of a plurality of receivers, said list of update keys allowing valid receivers to decrypt a valid content key using update keys obtained from the list of update keys;

generate a multiple nested list of decryption patterns based on the list of update keys;

broadcast said multiple nested list of decryption patterns to the plurality of receivers; and

recover a content key from the list of update keys by recovering an appropriate set of update keys for each receiver from the multiple nested list of decryption patterns and using the set of update keys to decrypt the content key, wherein the valid receivers receive the recovered content key to facilitate decryption of content, and each of the invalid receivers receives a distinct intermediate key to facilitate blocking of the content.

29.   (Currently Amended) The machine-readable medium of claim 28, wherein said ~~generating a~~ of the list of update keys comprises generating ~~at least one~~ one or more distinct intermediate ~~key~~ keys and ~~one~~ the content key.

30.   (Cancelled)

31.   (Cancelled)

32. (Currently Amended) The machine-readable medium of claim 28, wherein said generating a-of the multiple nested list of decryption patterns comprises encrypting an entry of the list of update keys using a key that is a combination of a previous update key, a secret keys-key for a receiver associated with the entry of the list of update keys, and an index indicating a location in said table of secret keys associated with each entry.

33. (Currently Amended) The machine-readable medium of claim 32, wherein an entry in said multiple nested list of decryption patterns includes a predetermined test pattern encrypted with the secret keys-key for a-the receiver associated with the entry of the list of update keys.

34. (Cancelled)

35. (Currently Amended) The machine-readable medium of claim 28, further comprising broadcasting said content encrypted with said content key.

36. (Original) The machine-readable medium of claim 35, further comprising decrypting said content encrypted with said content key using a content key recovered from the multiple nested list of decryption patterns.

Claims 37-45 (Cancelled)